80

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/048,216	04/25/2002	Jean-Sebastien Coron	032326-192	4787

21839 7590 07/06/2005

BUCHANAN INGERSOLL PC
(INCLUDING BURNS, DOANE, SWECKER & MATHIS)
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
CERVETTI, DAVID GARCIA	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 07/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/048,216	**Applicant(s)** CORON ET AL.	
	Examiner David G. Cervetti	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 January 2002*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *1/30/02*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Information Disclosure Statement

1. The listing of references in the specification is not a proper information disclosure statement. 37 CFR 1.98(b) requires a list of all patents, publications, or other information submitted for consideration by the Office, and MPEP § 609 A(1) states, "the list may not be incorporated into the specification but must be submitted in a separate paper." Therefore, unless the references have been cited by the examiner on form PTO-892, they have not been considered.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 5, 7, and 16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The term "small integer" in claims 5, 7, and 16 is a relative term which renders the claim indefinite. The term "small integer" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably appraised of the scope of the invention. The term “small integer” renders “t” indefinite.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. **Claim 3 is rejected under 35 U.S.C. 102(b) as being anticipated by Rueppel et al. (US Patent Number: 5,600,725).**

Regarding claim 3, Rueppel et al. tech an electronic signature method comprising a generation method and a signature verification method that comprises including part of the message inside the signature by suitably choosing the random data used during the generation of the signature (column 7, lines 50-67, column 8, lines 1-67, column 9, lines 1-10).

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. **Claim 4 is rejected under 35 U.S.C. 102(e) as being anticipated by Park et al. (US Patent Number: 5,966,445).**

Regarding claim 4, Park et al. tech an electronic signature method comprising a generation method and a signature verification method that comprises the steps of eliminating some of the bytes representing the signature, and reconstituting the signature during the verification phase (column 9, lines 30-67, column 10, lines 1-67, column 9, lines 1-10).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. **Claims 1-2, 5-19, 27-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rueppel et al., and further in view of Menezes et al. (NPL Handbook of Applied Cryptography).**

Regarding claim 1, Rueppel et al. teach an electronic signature method comprising a generation method and a verification method allowing total reconstitution of a message, said method utilizing a set having a group structure of order r, where r is a prime number, with a zero element denoted O and generating the point G, and employing a private key that is a positive integer less than r, and a public key being the point W=s.G, said method using a non-zero integer constant k, wherein the signature generation method includes the following four steps:

1) Generating a random number u between 1 and r-1 and calculating V=u.G;

2) Associating an integer i with the point V and calculating c = i + f modulo r; if c=0, returning to step 1;

3) Calculating the integer d=u^{-1} *(k+ s*c) modulo r; if d =0, returning to step 1; and

4) Utilizing the pair of integers (c, d) as the signature (column 1, lines 48-67, column 2, lines 1-50, column 7, lines 38-67, and column 8, lines 1-67);

and wherein the signature verification method includes the following six steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [1,r-1], the signature is not valid;

2) calculating the integers $h = d^{-1}$ modulo r, h_1 =k*h modulo r and h_2=c*h modulo r;

3) Calculating the point $P = h_1G + h_2W$; if P =0, the signature is not valid;

4) Associating an integer i with the point P;

5) Calculating the integer f = c-i modulo r; and

6) Finding the message m from f and verifying that f = R(m); if yes, the signature of the message m is valid; otherwise the signature is not valid (column 4, lines 1-67, column 5, lines 1-67, column 7, lines 38-67, column 8, lines 1-67).

Rueppel et al. do not disclose expressly using a redundancy function R. Rueppel et al. do teach using a redundancy check to determine if the signature and the message are genuine (column 5, lines 12-40). However, Menezes et al. teach using a suitable redundancy function to guard against existential forgery (page 461). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a redundancy function to guard against existential forgery with the system of Rueppel et al. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use redundancy to protect against forgery (Menezes et al., pages 426-435).

Regarding claim 2, Rueppel et al. teach an electronic signature method comprising a generation method and a signature verification method allowing partial reconstruction of a message, the message m to be signed being divided into two parts, the first part m_1 of constant size being reconstituted from the signature, the second part m_2 being transmitted with the signature of the method, said method utilizing a set having a group structure of order r, where r is a prime number, with a zero element denoted O and generating the point G, and employing a private key that is a positive integer less than r and a public key being the point W = s.G, wherein the method of generating the signature of a message m consisting of the messages m_1 and m_2 includes the following six steps:

1) Generating a random integer u between 1 and r-1 and calculating V =u.G;

2) Calculating $f_1 = R(m_1)$;

3) Associating an integer i with the point V and calculating $c = i+f_1$ modulo r; if c=0, returning to step 1;

4) Calculating $f_2 = H(m_2)$, where H is a hash function;

5) Calculating the integer $d = u^{-1} * (f_2 + s * c)$ modulo r; if d =0, returning to step 1; and

6) Utilizing the pair of integers (c, d) as the signature (column 1, lines 48-67, column 2, lines 1-50, column 7, lines 38-67, and column 8, lines 1-67);

and wherein the signature verification method takes as an input a pair of integers (c, d) and the partial message m_2 and comprises the following seven steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [1,r-1] , the signature is not valid;

2) Calculating $f_2 = H(m_2)$, where H is a hash function;

3) calculating the integers $h=d^{-1}$ modulo r, $h_1 = f_2*h$ modulo r and $h_2=c*h$ modulo r;

4) Calculating the point $P= h_1G + h_2W$; if P=0, the signature is not valid;

5) Associating the integer i with the point P;

6) Calculating the integer f_1 = c-i modulo r; and

7) Obtaining the message m_1 from f_1 and verifying that $f_1 =R(m_1)$; if yes, the signature of the message m is valid; otherwise the signature is not valid (column 4, lines 1-67, column 5, lines 1-67, column 7, lines 38-67, column 8, lines 1-67).

Rueppel et al. do not disclose expressly using a redundancy function R. Rueppel et al. do teach using a redundancy check to determine if the signature and the message are genuine (column 5, lines 12-40). However, Menezes et al. teach using a suitable redundancy function to guard against existential forgery (page 461). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a redundancy function to guard against existential forgery with the system of Rueppel et al. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use redundancy to protect against forgery (Menezes et al., pages 426-435).

Regarding claim 5, Rueppel et al. teach a generation method and a verification method in which part of the message of size t bytes is included in the integer d, t being a small integer, the signature being a pair of integers (c, d), the t least significant bytes of an integer g containing t bytes of the message, the said method using a set having a group structure of order r, where r is a prime number, with a zero element denoted O and generating the point G, and employing a private key that is a positive integer s less than r and a public key being the point W= s.G, wherein the method of generating the signature of a message m includes the following five steps:

2) Generating a random number u between 1 and r-1 and calculating V =u.G;

3) Associating an integer i with the point V and calculating c = i+f modulo r; returning to step 1 if c = 0.

4) Calculating the integer d=u-s*c modulo r; if d is not equal to m modulo 2^{8t}, returning to step 2; and

5) Utilizing the pair of integers (c, d) as the signature (column 1, lines 48-67, column 2, lines 1-50, column 7, lines 38-67, and column 8, lines 1-67);

and wherein the signature verification method includes the following five steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [0,r-1], the signature is not valid;

2) Calculating the point P= d.G + c.W; if P = 0, the signature is not valid;

3) Associating the integer i with the point P;

4) Calculating the integer f =c-i modulo r;

5) Obtaining the message m' from f and verifying that f =R(m'); if such is not the case, the signature is not valid; if such is the case, the signature is valid and the message m is the concatenation with the message m' of the t least significant bytes of the integer d (column 4, lines 1-67, column 5, lines 1-67, column 7, lines 38-67, column 8, lines 1-67).

Rueppel et al. do not disclose expressly using a redundancy function R and

1) Removing the t least significant bytes of the message m and storing the result in m'; calculating f = R(m'). Rueppel et al. do teach using a redundancy check to determine if the signature and the message are genuine (column 5, lines 12-40) and including part of the message (column 7, lines 50-67, column 8, lines 1-67, column 9, lines 1-10). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use some least significant bytes of a message during the signature generation step. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use a portion of a message to generate a digital signature to reduce the amount of data to transfer. However, Menezes et al. teach using a suitable redundancy function to guard against existential forgery (page 461). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a redundancy function to guard against existential forgery with the system of Rueppel et al. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use redundancy to protect against forgery (Menezes et al., pages 426-435).

Regarding claim 6, the combination of Rueppel et al. with Menezes et al. teaches the limitations as set forth under claim 5 above. Furthermore, Menezes et al. teach the preprocessing of the signature generation to accelerate the generation of the signatures, said method comprising a pretreatment phase and a signature generation phase, said pretreatment phase taking as an input a secret key s and putting in memory in a table a large number of values (i, x_u) with x_u =u-s*i modulo r and i being the integer associated with the point V=u.G, so that these values can be accessed by the remainder of x_u modulo 2^{8t} (pages 484-486), said signature generation phase utilizing a redundancy function R (page 461). Rueppel et al. teach a set having a group structure of order r, where r is a prime number, with a zero element denoted O and generating the point G, and employing a private key that is a positive integer s less than r and a public key being the point W = s.G, said signature generation phase comprising the following eight steps:

2) Calculating the integer y = s*f modulo r and the integer l=y modulo 2^{8t};

3) If y < r/2, first of all executing step 4 and next step 5; otherwise executing first of all step 5 and next step 4;

4) Accessing the elements of the table where the remainder modulo 2^{8t} is 1+d modulo 2^{8t} and selecting an element such that x_u is greater than or equal to y; if such an element exists, it is eliminated from the table and the method passes to step 6;

5) Accessing the elements of the table where the remainder modulo 2^{8t} is 1+d+r modulo 2^{8t} and selecting an element such that x_u is less than y; if such an element exists, it is eliminated from the table and the method passes to step 6;

6) Calculating the integer d =x_u-y modulo r;

7) Obtaining the integer i associated with x_u and calculating c = i+f modulo r; and

8) Utilizing the pair of integers (c, d) as the signature (column 1, lines 48-67, column 2, lines 1-50, column 7, lines 38-67, and column 8, lines 1-67).

Rueppel et al. do not disclose expressly 1) Removing the t least significant bytes of the message m and storing the result in m'; calculating f = R(m'), the t least significant bytes of the message m are stored in the integer d. Rueppel et al. do teach including part of the message (column 7, lines 50-67, column 8, lines 1-67, column 9, lines 1-10). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use some least significant bytes of a message during the signature generation step. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use a portion of a message to generate a digital signature to reduce the amount of data to transfer.

Regarding claim 7, the combination of Rueppel et al. with Menezes et al. teaches the limitations as set forth under claim 2 above. Furthermore, Rueppel et al. teach a signature generation method and a signature verification method, said method including part of the message of size t bytes in the integer d, t being a small integer, the t least significant bytes of the integer d containing t bytes of the message, said method utilizing a set having a group structure of order r, where r is a prime number, with a zero element denoted O and generating a point G, and employing a private key that is a positive integer less than r and a public key being the point W=s.G, wherein the method of generating the signature of a message m consisting of the messages m_1 and m_2 includes the following six steps:

1) Generating a random integer u between 1 and r-1 and calculating V =u.G;

2) Calculating f_1 =R(m_1);

3) Associating an integer i with the point V and calculating c=i+ f_1 modulo r; if c=0, returning to step 1;

4) Calculating f_2=H(m_2), where H is a hash function;

5) calculating the integer $d=u^{-1}*(f_2+s*c)$ modulo r; if d=0 or if d is not equal to m_2 modulo 2^{8t}, returning to step 1; and

6) Utilizing the pair of integers (c, d) as the signature, and the message to be transmitted is m'_2 consisting of m_2 deprived of its t least significant bytes (column 1, lines 48-67, column 2, lines 1-50, column 7, lines 38-67, and column 8, lines 1-67);

and wherein the signature verification method takes as an input a pair of integers (c, d) and the partial message m'_2 and comprises the following eight steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [1,r-1], the signature is not valid;

2) Making up m'_2 as m_2 by adding to it the t least significant bytes of d;

3) Calculating $f_2 =H(m_2)$, where H is a hash function;

4) Calculating the integers $h=d^{-1}$ modulo r, $h_1 = f_2 * h$ modulo r and $h_2 =c*h$ modulo r;

5) Calculating the point $P =h_1G+h_2W$; if P =0 the signature is not valid;

6) Associating the integer i with the point P;

7) Calculating the integer f_1 = c-i modulo r; and

8) Obtaining the message m_1 from f_1 and verifying that $f_1 =R(m_1)$; if yes, the signature of the message m is valid; otherwise the signature is not valid (column 4, lines 1-67, column 5, lines 1-67, column 7, lines 38-67, column 8, lines 1-67).

Rueppel et al. do not disclose expressly using a redundancy function R and

1) Removing the t least significant bytes of the message m and storing the result in m'; calculating f = R(m'). Rueppel et al. do teach using a redundancy check to

determine if the signature and the message are genuine (column 5, lines 12-40). However, Menezes et al. teach using a suitable redundancy function to guard against existential forgery (page 461). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a redundancy function to guard against existential forgery with the system of Rueppel et al. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use redundancy to protect against forgery (Menezes et al., pages 426-435).

Regarding claim 8, Rueppel et al. teach a method comprising a signature generation method and a signature verification method, said method being applied to the Nyberg and Rueppel signature scheme, wherein the signature generation method includes the following two steps:

1) Generating the signature of the message m using the Nyberg and Rueppel signature scheme, to obtain the pair of integers (c, d); and

2) Calculating d', the integer quotient of the division of the integer d by 2^{8t}; and utilizing the pair of integers (c, d') as the signature (column 1, lines 48-67, column 2, lines 1-50, column 7, lines 38-67, and column 8, lines 1-67, column 9, lines 1-10);

and wherein the signature verification method takes as an input a pair (c, d') and includes the following five steps:

1) If c does not belong to the interval [1,r-1], the signature is not valid;

2) Calculating the point $P=d'*2^{8t}.G+c.W$;

3) For j ranging from 0 to $2^{8t}-1$, executing the following steps:

3a) If P = O, executing step 3d);

3b) Associating the integer i with the point P and calculating the integer f=c-i modulo r;

3c) Finding the message m from f and verifying that f =R(m); if yes, executing step 5;

3d) Replacing P with P+G;

4) The signature is not valid and the method is terminated;

5) If the integer d=d'*2^{8t}+j does not belong to the interval [0,r-1], the signature is not valid; otherwise the signature is valid and the method is terminated (column 4, lines 1-67, column 5, lines 1-67, column 7, lines 38-67, column 8, lines 1-67).

Rueppel et al. do not disclose expressly a method that includes removing t bytes from a chain of bytes representing an integer d from a signature that is the pair of integers (c, d). Rueppel et al. do teach including part of the message (i.e. not all bytes from a chain of bytes) (column 7, lines 50-67, column 8, lines 1-67, column 9, lines 1-10). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use some least significant bytes of a message during the signature generation step. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use a portion of a message to generate a digital signature to reduce the amount of data to transfer.

Regarding claim 9, the combination of Rueppel et al. with Menezes et al. teaches the limitations as set forth under claim 2 above. Furthermore, Rueppel et al. teach a method comprising a signature generation method and a signature verification method, with partial reconstitution of a message according to Claim 2, wherein the signature generation method includes the following two steps:

1) Generating the signature of a message m using the signature scheme with partial reconstruction of the message according to claim 2, in order to obtain the pair of integers (c, d); and

2) Calculating d', the integer quotient of the division of the integer d by 2^{8t}; wherein the signature is the pair of integers (c, d') (column 1, lines 48-67, column 2, lines 1-50, column 7, lines 38-67, and column 8, lines 1-67, column 9, lines 1-10);

and wherein the modified signature verification method takes as an input a pair (c,d') and a message m_2 and includes the following two steps:

1) For i ranging from 0 to 2^{8t} -1 calculating the integer d=d'*2^{8t} +i and executing the signature verification method with partial reconstitution of the message according to claim 2, the signature to be verified being (c, d); if the signature verification method recognizes the signature (c, d) as valid, the signature is valid, and the method is terminated;

2) Otherwise the signature is not valid (column 4, lines 1-67, column 5, lines 1-67, column 7, lines 38-67, column 8, lines 1-67).

Rueppel et al. do not disclose expressly a method that includes removing t bytes from a chain of bytes representing an integer d from a signature that is the pair of integers (c, d). Rueppel et al. do teach including part of the message (i.e. not all bytes from a chain of bytes) (column 7, lines 50-67, column 8, lines 1-67, column 9, lines 1-10). Therefore, it would have been obvious to one having ordinary skill in the.art at the time the invention was made to use some least significant bytes of a message during the signature generation step. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use a portion of a message to generate a digital signature to reduce the amount of data to transfer.

Regarding claim 10, Rueppel et al. teach a method comprising a signature generation method and a signature verification method, said method utilizing a set having a group structure of order r, where r is a prime number, with a zero element denoted O and generating the point G, and employing a private key that is a positive integer s less than r and a public key being the point $W=s.G$, wherein the method of generating the signature of a message m includes the following five steps:

1) Generating a random number u and calculating $V=u.G$;

2) Obtaining the message m' by removing from the message m the t least significant bytes and calculating $f=R(m')$;

3) Associating an integer i with the point V and calculating $c= i+f$ modulo r; returning to step 1 if $c= 0$ and if i is not equal to m modulo 2^{8t};

4) Calculating $d=u-s*c$ modulo r; and

5) Utilizing the pair of integers (c, d) as the signature (column 1, lines 48-67, column 2, lines 1-50, column 7, lines 38-67, and column 8, lines 1-67);

and wherein the signature verification method includes the following four steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [0,r-1], the signature is not valid;

2) Calculating the point $P=d.G+c.W$; if $P=O$, the signature is not valid;

3) Associating the integer i with the point P and calculating the integer f = c-i modulo r; and

4) Finding the message m' from f and verifying that f =R(m'); if yes, finding the message m by concatenating the t least significant bytes of i with the message m' . The signature of the message m is then valid; otherwise the signature is not valid (column 4, lines 1-67, column 5, lines 1-67, column 7, lines 38-67, column 8, lines 1-67).

Rueppel et al. do not disclose expressly using a redundancy function R. Rueppel et al. do teach using a redundancy check to determine if the signature and the message are genuine (column 5, lines 12-40). However, Menezes et al. teach using a suitable redundancy function to guard against existential forgery (page 461). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a redundancy function to guard against existential forgery with the system of Rueppel et al. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use redundancy to protect against forgery (Menezes et al., pages 426-435).

Regarding claim 11, the combination of Rueppel et al. with Menezes et al. teaches the limitations as set forth under claim 2 above. Furthermore, Rueppel et al. teach a a signature generation method and a signature verification method, and making it possible to increase by t bytes the size of the message m_1 reconstituted from the signature, t being an integer variable, said method utilizing a set having a group structure of order r, where r is a prime number, with a zero element denoted O and generating the point G, and employing a private key that is a positive integer less than r and a public key being the point W=s.G, wherein the method of generating the signature of a message m includes the following six steps:

1) Generating a random integer u between 1 and r-1 and calculating V=u.G;

2) Obtaining m'_1 by removing the t least significant bytes from the message m_1. Calculating $f_1 = R(m'_1)$;

3) Associating an integer i with the point V and calculating $c = i + f_1$ modulo r; if c =0 or if i is not equal to m_1 modulo 2^{8t}, returning to step 1;

4) Calculating $f_2 = H(m_2)$, where H is a hash function;

5) Calculating the integer $d = u^{-1} * (f_2 + s * c)$ modulo r; if d=0, returning to step 1; and

6) Utilizing the pair of integers (c, d) as the signature (column 1, lines 48-67, column 2, lines 1-50, column 7, lines 38-67, and column 8, lines 1-67);

and wherein the signature verification method takes as an input a pair of integers (c, d) and the partial message m_2 and comprises the following seven steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [1,r-1], the signature is not valid;

2) Calculating $f_2 = H(m_2)$, where H is a hash function;

3) Calculating the integers $h = d^{-1}$ modulo r, $h_1 = f_2 * h$ modulo r and $h_2 = c * h$ modulo r;

4) Calculating the point $P = h_1 G + h_2 W$; if P=O, this signature is not valid;

5) Associating the integer i with the point P;

6) Calculating the integer $f_1 = c - i$ modulo r; and

7) Obtaining the message m'_1 from f_1 and verifying that $f_1 = R(m'_1)$; if yes, obtaining m_1 by concatenating the t least significant bytes of the integer i with the message m'_1. The signature of the message m is then valid; otherwise the signature is not valid (column 4, lines 1-67, column 5, lines 1-67, column 7, lines 38-67, column 8, lines 1-67).

Rueppel et al. do not disclose expressly using a redundancy function R. However, Menezes et al. teach using a suitable redundancy function to guard against existential forgery (page 461). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a redundancy function to guard against existential forgery with the system of Rueppel et al. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use redundancy to protect against forgery (Menezes et al., pages 426-435).

Regarding claims 12 and 26, the combination of Rueppel et al. with Menezes et al. teaches the limitations as set forth under claims 11 and 10 respectively above. Furthermore, Menezes et al. teach preprocessing the calculations making it possible to increase performance, comprising the further step of putting in memory in a table the pairs of integers (u, i) so that these integers are accessible to the value of i modulo 2^{8t}, t being an integer parameter (pages 484-486).

Regarding claim 13, Rueppel et al. teach a method comprising a signature generation method and a signature verification method, the signature consisting of the pair of integers (c, d), wherein the signature generation method includes the following two steps:

1) Generating the signature of a message m using the Nyberg-Rueppel signature scheme in order to obtain the pair of integers (c, d); and

2) Calculating c', the integer quotient of the division of the integer c by 2^{8t}, and employing the pair of integers (c', d) as the signature (column 1, lines 48-67, column 2, lines 1-50, column 7, lines 38-67, and column 8, lines 1-67, column 9, lines 1-10);

and wherein the signature verification method takes as an input the pair of integers (c', d) and includes the following five steps:

1) If d does not belong to the interval [0,r-1], the signature is not valid;

2) Calculating the point P=d.G+c'*2^{8t}.W;

3) For j ranging from 0 to 2^{8t}-1, executing the following steps;

3a) If P=O, executing step 3d);

3b) Associating the integer i with the point P and calculating the integer f=c-i modulo r;

3c) Finding the message m from f and verifying that f =R(m); if yes, executing step 5;

3d) Replacing P by P+W;

4) The signature is not valid and the method is terminated;

5) If the integer c= c'*2^{8t}+j does not belong to the interval [1,r-1], the signature is not valid; otherwise the signature is valid and the method is terminated (column 4, lines 1-67, column 5, lines 1-67, column 7, lines 38-67, column 8, lines 1-67).

Rueppel et al. do not disclose expressly a method for improving the Nyberg and Rueppel signature scheme consisting in removing t bytes from an integer c, t being an integer variable. Rueppel et al. do teach including part of the message (i.e. not all bytes) (column 7, lines 50-67, column 8, lines 1-67, column 9, lines 1-10). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to remove some bytes from an integer c. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use a portion of a message to generate a digital signature to reduce the amount of data to transfer.

Regarding claim 14, Rueppel et al. teach a method comprising a signature generation method and a signature verification method, wherein the signature generation method comprises the following two steps:

1) Generating the signature of the message m, using the signature scheme with partial reconstitution of the message in order to obtain the pair of integers (c, d); and

2) Calculating c' the integer quotient of the division of the integer c by 2^{8t}; and utilizing the pair of integers (c', d) as the signature (column 1, lines 48-67, column 2, lines 1-50, column 7, lines 38-67, and column 8, lines 1-67, column 9, lines 1-10);

and wherein the signature verification method takes as an input a pair of integers (c', d) and a message m_2 and comprises the following eight steps:

1) If d does not belong to the interval [1,r-1], the signature is not valid;

2) Calculating $f_2 =H(m_2)$, where H is a hash function;

3) Calculating the integers $h =d^{-1}$ modulo r, $h_1 = f_2*h$ modulo r and $h_2 = c'*2^{8t}*h$ modulo r;

4) Calculating the point $P = h_1.G + h_2.W$;

5) Calculating the point $Z =h.W$;

6) For j ranging from 0 to 2^{8t}-1, executing the following steps:

6a) If P=O, executing step 6d);

6b) Associating the integer i with the point P and calculating the integer f_1=c-i modulo r;

6c) Finding the message m_1 from f_1 and verifying that f_1 =R(m_1); if yes, executing step 8,

6d) Replacing P with P+Z;

7) The signature is not valid and the method is terminated;

8) If the integer c =c'*2^{8t}+j does not belong to the interval [1,r-1], the signature is not valid; otherwise the signature is valid and the method is terminated (column 4, lines 1-67, column 5, lines 1-67, column 7, lines 38-67, column 8, lines 1-67).

Rueppel et al. do not disclose expressly a method according to claim 2 for improving the signature scheme with partial reconstitution of the message that includes the further step of removing t bytes from the integer c, t being an integer variable. Rueppel et al. do teach including part of the message (i.e. not all bytes) (column 7, lines 50-67, column 8, lines 1-67, column 9, lines 1-10). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to remove some bytes from an integer c. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use a portion of a message to generate a digital signature to reduce the amount of data to transfer.

Regarding claims 15 and 27, the combination of Rueppel et al. with Menezes et al. teaches the limitations as set forth under claims 1 and 2 respectively above.

Furthermore, Rueppel et al. teach a method according to claim 1 for modifying the signature scheme with partial reconstruction of the message comprising the further step of replacing the signature (c, d) with the signature (h_2, d) with h_2=c*d^{-1} modulo r (column 1, lines 48-67, column 2, lines 1-50, column 7, lines 38-67, and column 8, lines 1-67, column 9, lines 1-10).

Regarding claim 16, Rueppel et al. teach a method comprising a signature generation method and a signature verification method, the said method having the step of including part of a message of size t bytes in an integer d, the signature being the pair of integers (c, d), t being a small integer, the t least significant bytes of the integer d containing t bytes of the message, the said method utilizing a set having a group structure of order r, where r is a prime number, with a zero element denoted O and generating the point G, and employing a private key that is a positive integer s less than r and a public key being the point W= s.G, wherein the method of generating the signature of a message m using the integer parameters t, a and k includes the following seven steps:

1) Calculating h = H(m), H being a hash function;

3) Storing as f the result of the concatenation with m' of the a most significant bytes of h;

4) Generating a random number u between 1 and r-1 and calculating V = u.G;

5) Associating an integer i with the point V and calculating c = i + f modulo r; returning to step 4 if c =0;

6) Calculating the integer d=u-s*c modulo r; if d is not equal to m modulo 2^{8t} returning to step 4; and

7) Utilizing the pair of integers (c, d) as the signature (column 1, lines 48-67, column 2, lines 1-50, column 7, lines 38-67, and column 8, lines 1-67);

and wherein the signature verification method includes the following seven steps:

1) If c does not belong to the interval [1,r-1] or if d does not belong to the interval [0,r-1], the signature is not valid;

2) Calculating the point P= d.G +c.W; if P = O, the signature is not valid;

3) Associating the integer i with the point P;

4) Calculating the integer f = c-i modulo r;

5) Concatenating the t least significant bytes of d with the message m' obtained from f by removing the a least significant bytes;

6) For b ranging from 0 to 2^{8k}-1 repeating the following step:

6a) Concatenating the message m' with b in order to obtain m and calculating h =H(m); verifying that the a most significant bytes of h and the a least significant bytes of f are identical; if yes, the signature of the message m is valid and the method is terminated;

7) Otherwise the signature is not valid (column 4, lines 1-67, column 5, lines 1-67, column 7, lines 38-67, column 8, lines 1-67).

Rueppel et al. do not disclose expressly

2) Removing the t least significant bytes and the k most significant bytes of the message m and storing the result in m'. Rueppel et al. do teach including part of the message (column 7, lines 50-67, column 8, lines 1-67, column 9, lines 1-10).

However, Menezes et al. teach including part of a message for partial message recovery (page 660). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use some least significant bytes and some most significant bytes of a message during the signature generation step. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to use a portion of a message to generate a digital signature to reduce the amount of data to transfer.

Regarding claims 17 and 28, the combination of Rueppel et al. with Menezes et al. teaches the limitations as set forth under claims 1 and 2 respectively above. Furthermore, Rueppel et al. teach a method for generating and verifying an electronic signature according to claim 1, wherein the operations are effected on an elliptic curve forming a group structure and having at least one point G, which is the generator of a sub-group of order r (column 1, lines 48-67, column 2, lines 1-50, column 7, lines 38-67, column 8, lines 1-67, and column 9, lines 1-10).

Regarding claim 18 and 29, the combination of Rueppel et al. with Menezes et al. teaches the limitations as set forth under claims 1 and 2 respectively above. Furthermore, Rueppel et al. teach a method for generating and verifying an electronic signature according to claim 1, wherein the operations are effected in the multiplicative group of the integers modulo a prime number p (column 1, lines 48-67, column 2, lines 1-50, column 9, lines 1-10).

Regarding claim 19 and 30, the combination of Rueppel et al. with Menezes et al. teaches the limitations as set forth under claims 1 and 2 respectively above. Furthermore, Rueppel et al. teach a method for generating and verifying an electronic signature according to claim 1, wherein the operations are effected in a multiplicative sub-group of order r of the multiplicative group of the integers modulo a prime number p with r dividing p-1 (column 1, lines 48-67, column 2, lines 1-50, column 9, lines 1-10).

10. Claims 20-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rueppel et al. and Menezes et al. as applied to claim 1 above, and further in view of Jaffe et al. (US Patent Number: 6,510,518).

Regarding claim 20, the combination of Rueppel et al. with Menezes et al. does not disclose expressly wherein said device is a portable device. However, Jaffe et al. teach generating electronic signatures using a portable device (column 16, lines 63-67, column 17, lines 1-34). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the method of Rueppel et al. and Menezes et al. on a portable device. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to generate digital signatures with portable devices.

Regarding claim 21, the combination of Rueppel et al. with Menezes et al. does not disclose expressly wherein the device is a smart card. However, Jaffe et al. teach generating electronic signatures using a smart card (column 16, lines 63-67, column 17, lines 1-34). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the method of Rueppel et al. and Menezes et al. on a smart card. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to generate digital signatures with smart cards.

Regarding claim 22, the combination of Rueppel et al. with Menezes et al. does not disclose expressly wherein the device is a contact-less card. However, Jaffe et al. teach generating electronic signatures using a contact-less card (column 16, lines 63-67, column 17, lines 1-34). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the method of Rueppel et al. and Menezes et al. on a contact-less card. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to generate digital signatures with contact-less cards.

Regarding claim 23, the combination of Rueppel et al. with Menezes et al. does not disclose expressly wherein the device is a PCMCIA card. However, Jaffe et al. teach generating electronic signatures using a PCMCIA card (column 16, lines 63-67, column 17, lines 1-34). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the method of Rueppel et al. and Menezes et al. on a contact-less card. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to generate digital signatures with PCMCIA card.

Regarding claim 24, the combination of Rueppel et al. with Menezes et al. does not disclose expressly wherein the device is a badge. However, Jaffe et al. teach generating electronic signatures using a badge (column 16, lines 63-67, column 17, lines 1-34). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the method of Rueppel et al. and Menezes et al. on a badge. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to generate digital signatures with badges.

Regarding claim 25, the combination of Rueppel et al. with Menezes et al. does not disclose expressly wherein the device is an intelligent watch. However, Jaffe et al. teach generating electronic signatures using a portable device (column 16, lines 63-67, column 17, lines 1-34). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the method of Rueppel et al. and Menezes et al. on an intelligent watch since it is a portable device. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to generate digital signatures with portable devices.

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DGC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100